Security Management & Organization

Corporate Security Organization

Exercise 6.1 (🤝/📌)

1. Brainstorm security roles and teams in the organizations you work for.

2. Associate tasks and responsibilities with these roles.

3. Where are these roles/teams located within your organization?

Job Titles/Description Summaries

- **Security Analyst**: analyzes and assesses vulnerabilities in the infrastructure (software, hardware, networks), investigates available tools and countermeasures to remedy the detected vulnerabilities, and recommends solutions and best practices. Analyzes and assesses damage to the data/infrastructure as a result of security incidents, examines available recovery tools and processes, and recommends solutions. Tests for compliance with security policies and procedures. May assist in the creation, implementation, and/or management of security solutions.

- **Security Engineer**: Performs security monitoring, security and data/logs analysis, and forensic analysis, to detect security incidents, and mounts incident response. Investigates and utilizes new technologies and processes to enhance security capabilities and implement improvements.

- **Security Architect**: Designs a security system or major components of a security system, and may head a security design team building a new security system.

- **Security Administrator**: Installs and manages organization-wide security systems. May also take on some of the tasks of a security analyst in smaller organizations.

- **Security Software Developer**: Develops security software, including tools for monitoring, traffic analysis, intrusion detection, virus/spyware/malware detection, anti-virus software, and so on. Also integrates/implements security into applications software.

- **Cryptographer/Cryptologist**: Uses encryption to secure information or to build security software. Also works as researcher to develop stronger encryption algorithms.

- **Cryptanalyst**: Analyzes encrypted information to break the code/cipher or to determine the purpose of malicious software.

- **Chief Information Security Officer**: a high-level management position responsible for the entire information security division/staff. The position may include hands-on technical work.

- **Security Consultant/Specialist**: Broad titles that encompass any one or all of the other roles/titles, tasked with protecting computers, networks, software, data, and/or information systems against viruses, worms, spyware, malware, intrusion detection, unauthorized access, denial-of-service attacks, and an ever increasing list of attacks by hackers acting as individuals or as part of organized crime or foreign governments.

Very Specialized Roles

- **Intrusion Detection Specialist**: Monitors networks, computers, and applications in large organizations, looking for events and traffic indicators that signal intrusion. Determines the damage caused by detected intrusions, identifies how an intrusion occurred, and recommends safeguards against similar intrusions. Also does penetration testing to identify vulnerabilities and recommend safeguards as preemptive measures.

- **Computer Security Incident Responder**: A member of team that prepares for and mounts rapid response to security threats and attacks such as viruses and denial-of-service attacks.

- **Source Code Auditor**: Reviews software source code to identify potential security issues and vulnerabilities that could be exploited by hackers to gain unauthorized access to data and system resources.

- **Virus Technician**: analyzes newly discovered computer viruses, and designs and develops software to defend against them.

- **Penetration Tester** (also known as Ethical Hacker or Assurance Validator): Not only scans for and identifies vulnerabilities, but exploits them to provide hard evidence that they are vulnerabilities. When penetration-testing, large infrastructures such as power grids, utility systems, and nuclear facilities, large teams of penetration testers, called Red Teams, are employed.

- **Vulnerability Assessor**: Scans for, identifies and assesses vulnerabilities in IT systems including computers, networks, software systems, information systems, and applications software.

Cyber Incident Response Team (CIRT)

Also known as a "computer incident response team," this group is responsible for responding to security breaches, viruses and other potentially catastrophic incidents in enterprises that face significant security risks. In addition to technical specialists capable of dealing with specific threats, it should include experts who can guide enterprise executives on appropriate communication in the wake of such incidents. The CIRT normally operates in conjunction with other enterprise groups, such as site security, public-relations and disaster recovery teams. [^1]

Six steps for effective Incident Response

1. **Preparation**: helps organizations determine how well their CIRT will be able to respond to an incident and should involve policy, response plan/strategy, communication, documentation, determining the CIRT members, access control, tools, and training

2. **Identification**: process through which incidents are detected, ideally promptly to enable rapid response and therefore reduce costs and damages

3. **Containment**: contain the damage and prevent further damage from occurring

4. **Eradication**: effective incident response that entails removing the threat and restoring affected systems to their previous state

5. **Recovery**: testing, monitoring, and validating systems while putting them back into production in order to verify that they are not re-infected or compromised

6. Lessons Learned

Lessons learned is a critical phase of incident response because it helps to educate and improve future incident response efforts. This is the step that gives organizations the opportunity to update their incident response plans with information that may have been missed during the incident, plus complete documentation to provide information for future incidents. Lessons learned reports give a clear review of the entire incident and may be used during recap meetings, training materials for new CIRT members, or as benchmarks for comparison.

Security Operations Center (SOC)

> A security operations center (SOC) is a facility that houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis. The SOC team's goal is to detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes. Security operations centers are typically staffed with security analysts and engineers as well as managers who oversee security operations. SOC staff work close with organizational incident response teams to ensure security issues are addressed quickly upon discovery. [^2]

Security Awareness

Security Awareness

Security awareness is a formal process for training and educating employees about IT protection. It involves:

- Programs to educate employees
- Individual responsibility for company security policies
- Measures to audit these efforts [^3]

Stages of Security Awareness

1. Determining the current status

2. Developing and crafting a security awareness program

3. Deploying said program to employees

4. Measuring the progress made by the program and revising as necessary [^3]

Exercise 6.2

1. Does your organization have a Security Awareness program?

2. What kinds of activities or trainings are employed?

3. How are these trainings conducted with the employees?

4. Are there dedicated employee groups who receive any special trainings?

5. Read and make up your own opinion on Bruce Schneier's article On Security Awareness Training (🏠)

Security Standards & Regulations

ISO 27001

ISO 27001 is an international standard published by the International Standardization Organization (ISO), and it describes how to manage information security in a company. The latest revision of this standard was published in 2013, and its full title is now ISO/IEC 27001:2013. The first revision of the standard was published in 2005, and it was developed based on the British standard BS 7799-2. [[^4]

ISO 27001 Controls (Annex A)

- A.5 **Information security policies** – controls on how the policies are written and reviewed

- A.6 **Organization of information security** – controls on how the responsibilities are assigned; also includes the controls for mobile devices and teleworking

- A.7 **Human resources security** – controls prior to employment, during, and after the employment

- A.8 **Asset management** – controls related to inventory of assets and acceptable use, also for information classification and media handling [^5]

- A.9 **Access control** – controls for Access control policy, user access management, system and application access control, and user responsibilities

- A.10 **Cryptography** – controls related to encryption and key management

- A.11 **Physical and environmental security** – controls defining secure areas, entry controls, protection against threats, equipment security, secure disposal, clear desk and clear screen policy, etc.

- A.12 **Operational security** – lots of controls related to management of IT production: change management, capacity management, malware, backup, logging, monitoring, installation, vulnerabilities, etc. [^5]

- A.13 **Communications security** – controls related to network security, segregation, network services, transfer of information, messaging, etc.

- A.14 **System acquisition, development and maintenance** – controls defining security requirements and security in development and support processes

- A.15 **Supplier relationships** – controls on what to include in agreements, and how to monitor the suppliers

- A.16 **Information security incident management** – controls for reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence [^5]

- A.17 **Information security aspects of business continuity management** – controls requiring the planning of business continuity, procedures, verification and reviewing, and IT redundancy

- A.18 **Compliance** – controls requiring the identification of applicable laws and regulations, intellectual property protection, personal data protection, and reviews of information security [^5]

⚠️ *[...] while IT is certainly important, IT alone cannot protect information. Physical security, legal protection, human resources management, organizational issues – all of them together are required to secure the information.* [^5]

ISO 27002

> ISO/IEC 27002 provides best practice recommendations on information security controls for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS). Information security is defined within the standard in the context of the C-I-A triad. [^6]

CIS Controls

- Maintained by the Center for Internet Security

- 20 prioritized actions to beat the vast majority of the most common attacks

- Mappings to regulatory and compliance frameworks are available

ℹ️ *An overview with regulatory framework mappings is available as a poster in its 41st edition (Winter 2016).*

CIS Controls™ V7

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols, and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

Other Standards (Examples)

- NIST 800-53 (Security and Privacy Controls for Information Systems and Organizations)

- DHS CDM Program

- PCI DSS

- BSI IT-Grundschutz-Standards

- BSI-Kritisverordnung (🇩🇪)

Security Communities & Associations

ISSA

ISSA is the community of choice for international cybersecurity professionals dedicated to advancing individual growth, managing technology risk and protecting critical information and infrastructure.

The **Information Systems Security Association (ISSA)®** is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

ISACA

[...] **ISACA**® is a global association helping individuals and enterprises achieve the positive potential of technology. Today's world is powered by technology, and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations.

ISACA leverages the expertise of its 450,000 engaged professionals in information and cyber security, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology

(ISC)²

> **(ISC)²** is an international, nonprofit membership association for information security leaders like you. We're committed to helping our members learn, grow and thrive. More than 138,000 certified members strong, we empower professionals who touch every aspect of information security.

Computer Security Certifications

Abbr.	Title	Issuer
CISSP	Certified Information Systems Security Professional	(ISC)²
SSCP	Systems Security Certified Practitioner	(ISC)²
CSSLP	Certified Secure Software Lifecycle Professional	(ISC)²
CISM	Certified Information Security Manager	ISACA
OSCP	Offensive Security Certified Professional	Offensive Security

💰 *Security certifications typically come with an exam cost and an annual renewal fee.*

SANS Institute

The **SANS Institute** was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. A range of individuals [...] are sharing the lessons they learn and are jointly finding solutions to the challenges they face. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community.

SANS is the most trusted and by far the largest source for information security training and security certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - the Internet Storm Center.

Useful SANS Resources

- Posters, e.g.
    - Security Leadership Poster
    - Security Awareness Roadmap
    - Secure DevOps Toolchain and SWAT Checklist (🔭)
- Information Security Policy Templates
- Incident Handler's Handbook
- **Internet Storm Center**

OWASP

> The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

🔭 *OWASP will be covered in detail next semester. The AppSec lectures of this course will be largely based on OWASP resources.*

OSSF

The OpenSSF brings together open source security initiatives under one foundation to accelerate work through cross-industry support. This is beginning with the Core Infrastructure Initiative and the Open Source Security Coalition, and will include new working groups that address vulnerability disclosures, security tooling and more.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Exercise 6.3 (🏠)

1. Download the Thresholds of the BSI-Kritis Ordinance

2. Check if your employer's industry is affected by BSI-Kritis at all

3. Calculate (or estimate) if your employer is above or below the defined threshold for BSI-Kritis for your industry